Chapter XLIV
An MDA Compliant Approach for Designing Secure Data Warehouses

Rodolfo Villarroel
Universidad Católica del Maule, Chile

Eduardo Fernández-Medina
Universidad de Castilla-La Mancha, Spain

Juan Trujillo
Universidad de Alicante, Spain

Mario Piattini
Universidad de Castilla-La Mancha, Spain

ABSTRACT
This chapter presents an approach for designing secure Data Warehouses (DWs) that accomplish the conceptual modeling of secure DWs independently from the target platform where the DW has to be implemented, because our complete approach follows the Model Driven Architecture (MDA) and the Model Driven Security (MDS). In most of real world DW projects, the security aspects are issues that usually rely on the DBMS administrators. We argue that the design of these security aspects should be considered together with the conceptual modeling of DWs from the early stages of a DW project, and being able to attach user security information to the basic structures of a Multidimensional (MD) model. In this way, we would be able to generate this information in a semi or automatic way into a target platform and the final DW will better suits the user security requirements.

INTRODUCTION
The goal of information confidentiality is to ensure that users can only access to the information that they are allowed. In the case of multidimensional (MD) models, confidentiality is crucial, because business information that is very sensitive, can be discovered by executing a simple query. Several papers deal with the importance of security in the software development process. Ghosh, Howell, and Whittaker (2002) state that security must influence all aspects of design, implementation, and software tests. Hall and Chapman
(2002) put forward ideas about how to build correct systems that fulfill not only the normal requirements but also the security ones. Nevertheless, security in databases and data warehouses is usually focused on the secure data storage, and not on their design. Thus, a methodology of data warehouse design based on the UML, with the addition of security aspects, would allow us to design DWs with the syntax and power of UML and with the new security characteristics ready to be used whenever the application has security requirements that demand them.

In this chapter, we present an approach for designing secure DWs as follows: we define the Model Driven Architecture (MDA) and Model Driven Security (MDS) compliant architecture of our approach, and we provide an Access Control and Audit (ACA) model for the conceptual MD modeling. Then, we extend the Unified Modeling Language (UML) with this ACA model, representing the security information (gathered in the ACA model) in the conceptual MD modeling, thereby allowing us to obtain secure MD models. By using this approach, makes possible to implement the secure MD models with any of the DBMS that are able to implement multilevel databases, such as Oracle Label Security and DB2 Universal Database, UDB.

The remainder of this chapter is structured as follows: Next section introduces related work; next, we present the MDA and MDS compliant architecture of our approach. Finally, we present the main conclusions.

**RELATED WORK**

As this chapter treats different research topics, the related work is organized as follows.

**Multidimensional Modeling**

Lately, several MD data models have been proposed. Some of them fall into the logical level (such as the well-known star-schema (Kimball & Ross, 2002). Others may be considered as formal models as they provide a formalism for the consideration of the main MD properties. A review of the most relevant logical and formal models can be found in Blaschka, Sapia, Höfling, and Dinter (1998) and Abelló, Samos, and Saltor (2001).

In this section, we will only make brief reference to the most relevant models that we consider “pure” conceptual MD models. These models provide a high level of abstraction for the main MD modeling properties at the conceptual level and are totally independent from implementation issues. One outstanding feature provided by these models is that they provide a set of graphical notations (such as the classical and well-known Extended Entity-Relationship model) which facilitates their use and reading. These are as follows: *The Dimensional-Fact (DF) Model* by Golfarelli, Maio, and Rizzi (1998), *The Multidimensional/ER (M/ER) Model* by Sapia, Blaschka, Höfling, and Dinter (1998), *The starER Model* by Tryfona, Busborg, and Christiansen (1999), *The Yet Another Multidimensional Model (YAM)* by Abelló et al. (2001), and the model proposed by Trujillo, Palomar, Gómez, and Song (2001). Unfortunately, none of these approaches for MD modeling considers security as an important issue in their conceptual models, and consequently they do not solve the problem of modeling security from the early stages of a DW project.

**Security Integration into the Design Process**

There are a few proposals which attempt to integrate security into conceptual modeling, such as the Semantic Data Model for Security (Smith, 1991) and the Multilevel Object Modeling Technique (Marks & Sell, 1996), but they are partial (since they do not cover the complete development process). More recent proposals are UMLSec (Jürjens, 2002) and SecureUML (Lodderstedt, Basin, & Doser, 2002) where UML is extended to develop secure systems. These approaches are interesting, but they only deal with information systems (IS) in general, whilst conceptual database and DW design are not considered. Moreover, a methodology and a set of models have been proposed (Fernández-Medina & Piattini, 2003) in order to design secure databases for implementation with Oracle9i Label Security (OLS). This approach, based on the UML, is relevant because it considers security aspects in all stages of the database development process, from requirement-gathering to implementation. Together with the previous methodology, the proposed Object Security Constraint Language (OCSCL), based on the Object Constraint Language (OCL) of UML, allows us to specify security constraints in the conceptual and logical database design process, and to implement them in a specific database management system (DBMS), OLS. Nevertheless, the previous methodology and models do not consider the design of secure MD mod-
Related Content

Certification and Security Issues in Biomedical Grid Portals: The GRISSOM Case Study
www.igi-global.com/chapter/certification-security-issues-biomedical-grid/46882?camid=4v1a

Protecting Patient Information in Outsourced Telehealth Services: Bolting on Security when it cannot be Baked in
www.igi-global.com/article/protecting-patient-information-outsourced-telehealth/2487?camid=4v1a

Trustworthy Networks, Authentication, Privacy, and Security Models
www.igi-global.com/chapter/trustworthy-networks-authentication-privacy-security/22049?camid=4v1a

Fuzzy Quantitative and Semi-Qualitative Risk Assessment in Projects
www.igi-global.com/article/fuzzy-quantitative-and-semi-qualitative-risk-assessment-in-projects/128961?camid=4v1a